REMARKS

Initially, Applicants would like to thank the Examiner for fully considering and accepting as persuasive the arguments submitted with the Response filed on January 30, 2007.

In the outstanding Office Action, claims 1-4, 6-9,11-14,16-19,21-24,and 26-30 were rejected under 35 U.S.C. §102(e) over SPIES et al. (U.S. Patent No. 5,689,565). Claims 5, 10, 15, 20, 25, and 31 were rejected under 35 U.S.C. §103(a) over SPIES in view of CORDERY et al. (U.S. Patent No. 5,796,841).

Respectfully, Applicants traverse each of the outstanding rejections. In this regard, SPIES is directed to a system and method to protect sensitive cryptographic keys and prevent unauthorized access to documents and instruments in electronic commerce transactions. In particular, at column 3, lines 6-9, SPIES discloses "[t]*his invention provides a cryptographic system and method that* ***protect a user's keys and prevents undesired access*** *and use of cryptographic functions without authorization from the user*" (emphasis added). Further, at column 5, lines 7-11, "***aspects of this invention are described in the context of an electronic commerce system*** *which facilitates the* ***secure interchange of commercial documents and instruments*** *over an insecure communication system*" (emphasis added).

Applicants traverse the rejection of independent claims 1 and 21. In this regard, the Office Action asserts that SPIES discloses features recited in independent claims 1 and 21 at Fig. 2, reference numbers 40, 42, 46, and 49, and at column 16, lines 31-42. Regarding reference number 40, SPIES states at column 7, lines 10-12, "[t]***he document(s) and instrument(s) are both encrypted and sent together over a communication path 40 to the computing unit 24(b) at the first recipient participant 22(b)***", and at column 6, lines 61-64, "[a]*s shown in FIG. 2, the* *transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority*** " (emphasis added). However, SPIES does not disclose a confirmation request system that generates a request for a confirmation receipt from a third party authenticator authenticating the attributes of a file, as recited in independent claim 1, or the related features of independent claim 21.

Further, at column 7, lines 20-24, SPIES discloses "[t]*he first recipient computing unit 24(b) then* ***passes the other(s) of the commerce document(s) 36 or the commerce instrument(s) 38 in encrypted form over a communication path 42*** *to a second computing unit 24(c) at the second recipient participant 22(c)* ", and at column 7, lines 46-50, "[a]*ssuming* ***the second participant 22(c)*** *can satisfy the commerce instrument, the computing unit 24(c)* ***returns a signed authorization receipt 44 over communication path 46 to the first recipient participant 22(b) indicating that payment is guaranteed*** " (emphasis added). However, the above-noted disclosure in SPIES is not a transferring system that transfers attributes of at least one file to be authenticated to the third party authenticator from the device that requested the confirmation, as recited in independent claim 1, or the related features of claim 21.

At column 7, lines 50-53, SPIES discloses "[t]*he* ***first recipient computing unit*** *24(b) then* ***sends a signed purchase receipt 48 over communication path 49*** *to the originating computing unit 24(a)* ", and at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority*** " (emphasis added). However, the cited portion of SPIES does not disclose a receiving system that receives the confirmation receipt comprising authenticated file attributes, after authentication by the third party authenticator, as recited in independent claim 1, or the related features recited in independent claim 21.

Additionally, at column 16, lines 31-42, SPIES discloses "[e]*ach computing unit 24(a)-24(c), as well as the credential server 28, is equipped to perform cryptographic functions including encryption, decryption, digital signing, and verification. The computing units are programmed to execute a commerce application that facilitates the computerized, electronic commerce system. To sustain the security and authentication functions of the electronic commerce system,* ***the commerce application must be able to provide encryption, decryption, and digital signing.*** *Accordingly,* ***each computing unit is implemented with a cryptography system that supports the commerce application with respect to these functions***" (emphasis added). However, this cited disclosure of SPIES does not teach that at least one file authentication is received from the third party authenticator, as recited in independent claims 1 and 21. Accordingly, in light of the forgoing, Applicants respectfully request reconsideration and withdrawal of the rejection of independent claims 1 and 21.

Applicants separately traverse the rejection of dependent claims 2 and 22. The Office Action asserts that SPIES discloses the features of dependent claims 2 and 22 at Fig. 2, reference numbers 32(a) and 32(b). However, the teachings of SPIES are not directed to third party authentication of a file received by a device, as recited in dependent claim 2, or the related features recited in dependent claim 22. Rather, SPIES teaches at column 12, lines 60-67 and Fig. 2 that participant credentials 32(a) and 32(b) are exchanged along with commerce documents and instruments among the transaction participants, and at column 11, lines 24-27 that "*the transaction process involves communication only among the participants*" and "[t]*here is* ***no***

interaction between any of the participants and the trusted credential authority (emphasis added)*"*. Thus, SPIES teaches that there is no involvement of the trusted credential authority after the initial registration that produces the credentials for the participants, and not that at least one file to be authenticated by a third party authenticator was received by the device as a file transfer from another device. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 2 and 22.

Applicants separately traverse the rejection of dependent claims 3 and 23. The Office Action asserts that features recited in dependent claims 3 and 23 are disclosed in SPIES at column 6, lines 44-59. SPIES discloses at column 6, lines 44-49, *"*[d]*uring the registration process (Fig. 1), the* ***computing units 24(a)-24(c)*** *at the participants 22(a)-22(c)* ***are each programmed to generate and send a registration packet*** *over the communication system (as represented by communication paths 30(a)-30(c))* ***to the credential binding server 28 at the trusted credential authority 26****. The credential binding server 28 is programmed to* ***produce unique credentials for each participant based upon their registration packets****"* (emphasis added). However, at column 8, lines 24-28, SPIES discloses *"the registration packet includes* ***identification information (name, location, etc.)****, public* ***cryptography keys*** *unique to the participant, and a* ***digital signature*** *of the participant"* (emphasis added). Therefore, this portion of SPIES is directed only to creating credentials for participants based on information they provide, and not to authentication of the attributes of a file or to transferring an identification of a requesting device or user of the device along with file attributes to be authenticated by the trusted third party. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 3 and 23.

Applicants separately traverse the rejection of dependent claims 4, 8, 13, 18, 24, and 29. The Office Action asserts that features recited in these dependent claims are disclosed in SPIES at column 7, lines 1-17. However, this cited portion of SPIES does not address digitally signing a confirmation receipt containing file attributes, but rather at column 7, lines 7-8, "*checking the digital signature of the trusted credential authority*". Further, SPIES discloses at column 7, lines 46-54 that the [second] "*computing unit 24(c) returns a* ***signed authorization receipt*** *44... to the first recipient participant 22(b)* ***indicating that payment is guaranteed***" and "*the first recipient computing unit 24(b) then* ***sends a signed purchase receipt*** *48... to the originating computing unit 24(a)*" (emphasis added). Therefore, this disclosure in SPIES does not teach a system, method, or device in which the authentication comprises digitally signing the confirmation receipt containing file attributes. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 4, 8, 13, 18, 24, and 29.

Applicants traverse the rejection of independent claims 6 and 16. In this regard, the Office Action asserts that SPIES discloses features recited in independent claims 6 and 16 at Fig. 2, reference numbers 40, 42, 46, and 49, and at column 7, lines 1-17, and column 16, lines 31-42. However, the cited portions of SPIES are principally the same as those cited by the Office Action regarding independent claims 1 and 21. Thus, these portions of SPIES do not disclose processing requests for authentication of files in digital systems as in the invention to which independent claims 6 and 16 are directed, and there is no teaching in these portions of SPIES of transferring attributes of at least one file to be authenticated to the third party authenticator.

Regarding reference number 40, SPIES states at column 7, lines 8-13 "[t]*he originating computing unit 24(a) then generates commerce document(s) 36 and commerce instrument(s) 38* *that are appropriate for the type of commercial transaction*" and these are "***sent together over a communication path 40 to the computing unit 24(b) at the first recipient participant 22(b)***", and at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority***" (emphasis added). However, there is no disclosure of a receiving system that transfers attributes of at least one file to be authenticated to the third party authenticator from the device that requested the confirmation, as recited in independent claim 6, or the related features recited in independent claim 16.

Regarding reference numbers 42 and 46 and column 7, lines 1-17, SPIES states at column 7, lines 3-7 "*a computing unit 24(a) at the originating participant 22(a) is programmed to request and* ***receive the credentials of all intended recipient computing units*** *24(b) and 24(c)*" and "*verifies the credentials by checking the digital signature of the trusted credential authority*" (emphasis added). The credentials as disclosed by SPIES are not file attributes. Further, SPIES teaches at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority***" (emphasis added). However, the cited disclosure of SPIES does not teach a processing system that processes a confirmation receipt, the processing comprising a unique digital characterization of the file attributes, assuring at least in part tampering and modification detection, as recited in independent claims 6, or the related features recited in independent claim 16.

At column 7, lines 50-53, SPIES discloses "[t]***he first recipient computing unit*** *24(b) then* ***sends a signed purchase receipt 48 over communication path 49*** *to the originating* *computing unit 24(a)"*, and at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority"*** (emphasis added). However, this cited portion of SPIES does not disclose a sending system that sends the confirmation receipt comprising authenticated file attributes to the requesting device, after processing by the third party authenticator, as recited in independent claim 6, or the related features recited in independent claim 16.

Additionally, at column 16, lines 31-42, SPIES discloses "[e]*ach computing unit 24(a)-24(c), as well as the credential server 28, is equipped to perform cryptographic functions including encryption, decryption, digital signing, and verification. The computing units are programmed to execute a commerce application that facilitates the computerized, electronic commerce system. To sustain the security and authentication functions of the electronic commerce system,* ***the commerce application must be able to provide encryption, decryption, and digital signing. Accordingly, each computing unit is implemented with a cryptography system that supports the commerce application with respect to these functions"*** (emphasis added). However, this cited disclosure of SPIES does not teach that at least one file is authenticated by the third party authenticator, as recited in independent claims 6 and 16. Accordingly, in light of the forgoing, Applicants respectfully request reconsideration and withdrawal of the rejection of independent claims 6 and 16

Applicants separately traverse the rejection of dependent claims 7, 12, 17, and 28. The Office Action asserts that features recited in dependent claims 7, 12, 17, and 28 are disclosed in SPIES at column 6, lines 44-59. However, the cited portions of SPIES are essentially the same as those cited by the Office Action regarding dependent claims 3 and 23. Thus, these portions of SPIES do not disclose that an identification of at least one of the requesting device or user of the requesting device is transferred along with attributes of the at least one file to be authenticated. SPIES discloses at column 6, lines 44-49, "[d]*uring the registration process (Fig. 1), the* ***computing units 24(a)-24(c)*** *at the participants 22(a)-22(c)* ***are each programmed to generate and send a registration packet*** *over the communication system (as represented by communication paths 30(a)-30(c))* ***to the credential binding server 28 at the trusted credential authority 26****. The credential binding server 28 is programmed to* ***produce unique credentials for each participant based upon their registration packets****"* (emphasis added). Further, at column 8, lines 24-28, SPIES discloses *"the registration packet includes identification information (name, location, etc.), public cryptography keys unique to the participant, and a digital signature of the participant"*. However, this portion of SPIES is directed only to creating credentials for participants based on information they provide and not authentication of the attributes of a file. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 7, 12, 17, and 28.

Applicants separately traverse the rejection of dependent claims 9, 14, 19, and 30. The Office Action asserts that features recited in dependent claims 9, 14, 19, and 30 are disclosed in SPIES at column 11, lines 2-6. However, the credentials as disclosed by SPIES do not comprise a confirmation receipt containing file attributes nor do the validity dates disclosed by SPIES comprise a date and time of authentication of file attributes. In fact, there is no mention of file attributes at all in SPIES. Rather, the cited disclosure states, "[t]*he credential contains the participant's public signing key, public key exchange key, unique identifiers, validity dates,* *owner information, issuer information, and information about the participant*". Therefore, the cited disclosure in SPIES does not teach a confirmation receipt that incorporates at least the date and time of authentication, and an identification of at least the requesting device. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 9, 14, 19, and 30.

Applicants traverse the rejection of independent claims 11 and 26. In this regard, the Office Action asserts that SPIES discloses features recited in independent claims 11 and 26 at Fig. 2, reference numbers 40, 42, 46, and 49, and at column 7, lines 1-17, and column 16, lines 31-42. However, the cited portions of SPIES are essentially the same as those cited by the Office Action regarding independent claims 6 and 16. Thus, these portions of SPIES do not disclose processing requests for authentication of files in digital systems as in the invention to which independent claims 11 and 26 are directed. Additionally, there is no teaching in these portions of SPIES of transferring attributes of at least one file to be authenticated to the third party authenticator, nor processing by the third party authenticator of a confirmation receipt comprising authenticated file attributes.

Regarding reference number 40, SPIES states at column 7, lines 8-13 "[t]*he originating computing unit 24(a) then generates commerce document(s) 36 and commerce instrument(s) 38 that are appropriate for the type of commercial transaction*" and these are "***sent together over a communication path 40 to the computing unit 24(b) at the first recipient participant 22(b)***" and at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority***" (emphasis added). However, there is no disclosure of an originating file authentication device originating a request for a confirmation receipt from a third party authenticator, and transferring attributes of at least one file to be authenticated to the third party authenticator, as recited in independent claim 11, or the related features recited in independent claim 26.

Regarding reference numbers 42 and 46 and column 7, lines 1-17, SPIES states at column 7, lines 3-7 "*a computing unit 24(a) at the originating participant 22(a) is programmed to request and receive the credentials of all intended recipient computing units 24(b) and 24(c)*" and "*verifies the credentials by checking the digital signature of the trusted credential authority*". The credentials as disclosed by SPIES are not file attributes. Further, SPIES teaches at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority***" (emphasis added). However, the cited disclosure of SPIES does not teach a confirmation request processing device for processing a confirmation receipt by the third party authenticator, the processing comprising a unique digital characterization of the file attributes, assuring at least in part tampering and modification detection, as recited in independent claims 11, or the related features recited in independent claim 26.

At column 7, lines 50-53, SPIES discloses "[t]***he first recipient computing unit*** *24(b) then* ***sends a signed purchase receipt 48 over communication path 49*** *to the originating computing unit 24(a)", and* at column 6, lines 61-64, "[a]*s shown in FIG. 2, the transaction process involves communication among the participants to the transaction* ***without any interaction between the participants and the trusted credential authority***" (emphasis added). However, the cited portion of SPIES does not disclose a transferring device for transferring the confirmation receipt comprising authenticated file attributes, after processing by the third party authenticator, to the device that requested confirmation, as recited in independent claim 11, or the related features recited in independent claim 26.

Additionally, at column 16, lines 31-42, SPIES discloses "[e]*ach computing unit 24(a)-24(c), as well as the credential server 28, is equipped to perform cryptographic functions including encryption, decryption, digital signing, and verification. The computing units are programmed to execute a commerce application that facilitates the computerized, electronic commerce system. To sustain the security and authentication functions of the electronic commerce system,* ***the commerce application must be able to provide encryption, decryption, and digital signing.*** *Accordingly,* ***each computing unit is implemented with a cryptography system that supports the commerce application with respect to these functions***" (emphasis added). However, this cited disclosure of SPIES does not teach that the third party authenticator authenticates the attributes of the at least one file as requested by the device, as recited in independent claims 11 and 26. Accordingly, in light of the forgoing, Applicants request reconsideration and withdrawal of the rejection of independent claims 11 and 26.

Applicants separately traverse the rejection of dependent claim 27. The Office Action asserts that features recited in dependent claim 27 are disclosed in SPIES at column 28, lines 35-53. The cited portion of SPIES discloses "*an interactive network structure*" that may employ "*digital switching technologies*" comprising a "*multi-tier distribution system*" connecting "*multiple set-top boxes*", and does not mention transfer or receipt of a file to be authenticated by a third party authenticator, as recited in dependent claim 27. Accordingly, in light of the forgoing, Applicants request reconsideration and withdrawal of the rejection of dependent claim 27.

As set forth above SPIES does not disclose the features recited in Applicants' independent claims 1, 6, 11, 16, 21, and 26, whether SPIES is considered alone or in any proper combination with another document. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of each of independent claims 1, 6, 11, 16, 21, and 26, at least for each of the reasons set forth above. Each of dependent claims 2-5, 7-10, 12-15, 17-20, 22-25, and 27-31 is allowable at least for depending, directly or indirectly, from an allowable independent claim, as well as for additional reasons related to their own recitations (e.g., including those set forth above with respect to numerous of the dependent claims).

If there should be any questions regarding the above-captioned application or the present Response, any representative of the U.S. Patent and Trademark Office is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,
Maurice W. HAFF et al.

Joshua M. Povsner
Reg. #42,086

Stephen M. Roylance
Reg. No. 31,296

July 25, 2007
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191